Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The Costumer referred to as “data controller”

and

Health Group
CVR 30273893
Kongevejen 377
2840 Holte

the “data processor”

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1.Table of Contents

2.Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of Health Groups analysis and healthcare services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3.The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

4.The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5.Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6.Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement

HEALTH GROUP

measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7.Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor

engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8.Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9.Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

    a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure (‘the right to be forgotten’)
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor’s obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller’s obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller’s obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

    c. the data controller’s obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller’s obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10.Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor’s notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller’s obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to

assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

2. The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

   a. Medical records
   b. Billing information

   The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14.Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15.Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   Data processor

Name	Asta Rude Riis
Position	Chief Privacy Officer
Telephone	61 40 48 42
E-mail	asr@healthgroup.dk

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the agreement is for the data controller to use Health Group's solutions and associated services, including DigiHealth.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The data processor provides solutions and associated services to the data controller and collects, processes, and stores personal information through them.

A.3. The processing includes the following types of personal data about data subjects:

1. Health screening and Health Check:
    - Regular personal information: Full name, email address, and possibly phone number
    - Sensitive personal information: Height, gender, age, weight, cholesterol levels, long-term blood sugar, waist circumference, triglycerides, and VO2 max
    - Survey history and indication of risk group

2. APV (workplace assessments):
    - Questionnaire responses

3. Combination treatment:
    - Regular personal information: Full name, email address, and possibly phone number
    - Sensitive personal information: Health information of various kinds depending on what is disclosed during the consultation/s.

A.4. Processing includes the following categories of data subject:

1. The costumer
2. The customers employees

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Health Group generally stores personal data for as long as there is an active relationship between Health Group and you, where it is in your interest for Health Group to process the information. Information is deleted when this relationship ends. Deletion only occurs to the extent that Health Group does not have legal authority or other legitimate reasons for storing the information for longer periods (e.g., other rules apply to journaling).

Health Group also has several specific deletion procedures associated with our health platform, DigiHealth, which are described below:

- The user always has the option to delete data/reports on their own.

- The user always has the option to delete their entire profile on their own.
- If the user does not have a history with the company, their data is deleted after 30 days.
- Inactive users will have their data deleted after 26 months of inactivity. The user will be notified one month in advance.
- If the company's agreement with Health Group ends, the user's data will be deleted.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Vicorda A/S	37468835	Lejrvej 25, 3500 Værløse	DigiHealth
Enalyzer	25761618	Refshalevej 147, 1432 København	APV (workplace assesments)
Gecko Booking	29517096	Silkeborgvej 758, 8220 Aarhus	Booking
Techogym (Pedan)	46476417	Københavnsvej 244, 4600 Køge	Fitness

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor’s processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor receives lists of names and email addresses from the data controller for all employees in the company. The purpose of the employee list is:

a. Importing into DigiHealth for booking, information about health offers in the company, etc.
b. Sending out survey questionnaires through DigiHealth or Enalyzer (after agreement with the data controller).

C.2. Security of processing

The level of security shall take into account:

The data processor's solutions are generally based on the registered employees to provide information about their work, well-being, and own health (health information). The data processor has therefore ensured a high level of data security. The data processor is entitled and obliged to make decisions about which technical and organizational security measures should be used to create the necessary (and agreed) security level around the information.

The data processor is also entitled and obliged to make decisions about which technical and organizational security measures should be implemented to establish the necessary (and agreed) security level.

However, the data processor must - under all circumstances and as a minimum - implement the following measures, which have been agreed with the data controller:

The data processor ensures that data is stored securely and confidentially. The data processor's security measures are divided into organizational and technical measures. The organizational security measures mean that only trusted personnel with a legitimate purpose have access to personal data. The data processor's staff are guided and trained continuously in data security, including how to handle and protect information. A register of data processing activities (Article 30 register) is also kept.

The technical security measures relate to the use of IT systems for registration and administration. Data is stored securely and has the necessary level of protection.

Daily data backups are performed.

Internal IT systems and hardware are additionally protected by passwords, updated antivirus software, firewalls, two-factor authentication (2FA), and physical material is stored in a locked place. When disposing of or repairing hardware, care is taken to ensure that information cannot become known to unauthorized persons.

Logging of business-critical systems is performed.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The data processor shall, to the extent possible within the scope and extent below, assist the data controller in accordance with Provision 9.1 and 9.2 by implementing the following technical and organizational measures:

The data processor shall develop its own procedures for rights requests and security incidents that meet the requirements of the General Data Protection Regulation.

C.4. Storage period/erasure procedures

Personal data is stored for the duration of the contract (main agreement), after which it is deleted by the data processor. Employee profiles are automatically deleted if the employee has been inactive for 26 months.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- At the data processor at the data processors address
- At sub-data processors at the sub-data processors address

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not provide a documented instruction regarding the transfer of personal data to a third country in these provisions or subsequently, the data processor is not authorized to carry out such transfers within the framework of these provisions.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller (or their representative) is entitled to conduct written and/or physical inspections of the data processor's facilities and security measures to verify that the processing of personal data entrusted to the data processor is in accordance with these provisions. The following audits, including inspections, can be carried out:

The data controller may at any time request a copy of the annual independent audit (ISAE 3402 type 2) that declares compliance with these provisions.
The data controller is entitled, at their own expense, to have the data processor's processing of personal data subject to an annual audit by an independent third party or to otherwise conduct annual supervision of the data processor's processing of personal data. In connection with such an audit, the data controller is obliged to remunerate the data processor for the time expended.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

This clause outlines the obligations and responsibilities of the processor with regard to sub-processors. The processor must conduct inspections, both physical and written, of the facilities and security measures of its sub-processors to ensure that the processing of personal data by the sub-processors complies with the terms of these provisions. The processor may request written statements or revision declarations from its sub-processors, documenting that the processing of personal data is being carried out in compliance with these provisions. If a written statement is not satisfactory, the processor may conduct physical inspections of the sub-processor's facilities and security measures.

If the data controller requires the processor to conduct physical inspections of sub-processors, the data controller must reimburse the processor for the time and expenses incurred. If the data controller requests that the processor subject sub-processors to specific revisions, the data controller will be responsible for the costs associated with such revisions.

Furthermore, the data controller has the right to request documentation of the processor's inspections of its sub-processors.